Why hardening bios?

It is a good idea add a password to enter the BIOS. Why is that? Was is the worst that can happen?

Intel Active Management Technology (IAMT)

IAMT is a hardware and firmware technology used to perform out-of-band access to a computer. This means that if IAMT is enabled a user can remotely start the computer and then access that computer (if the user has credentials). How is it even possible to access a computer that is not even turned on, you might wonder. How can it have an IP if it is not turned on?

Intel add a separate microprocessor. It does not require an OS to work or any kind of locally installed agent.

AMT is most often found in business computers, and not as often on regular non-business computers.

IAMT is usually accessible over the network on the port 16992 or 16993 as a web interface.

Features

- One feature that is provided by IAMT is Keyboard-Video-Mouse (KVM) over LAN. This means that, if enabled, someone can access the computer over the network.
- Remote boot - you can remotely boot the computer from a different image. You can even boot from an image on a network share.

Risks

This means that if an attacker has physical access to a computer and bios password is not set, that person can enter into the BIOS and enable IAMT. If the disk is not encrypted the attacker can go back to anyware on the lan and then just boot the computer. If it requires a password to log in the attacker can bypass that simply by booting the computer from an image remote.

Change boot-order

If no BIOS password is set then an attacker can change the boot-order, in order to boot the computer from a USB. This way it is possible to bypass the OS authentication. If the computer is encrypted there is nothing that user can do.

Changing the boot-order is only an interesting attack